



Physical and Environmental Security Policy

DOC-IT-IS-11
Revision 2.1
NOVEMBER 1, 2025

This document contains proprietary information, which is the exclusive property of RXO, Inc. and may not be used or reproduced, in whole or in part, without the express permission of RXO, Inc.

Copyright © 2025 RXO, Inc. All rights reserved.

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<u>Rev.</u>	<u>Rev. Date</u>	<u>Revision Description</u>
1.0	11/01/2022	Initial Version
2.0	11/01/2024	Annual Review
2.1	11/01/2025	RXO, Inc updates, annual review

11.0 Physical and Environmental Security Policy	4
11.0.1 Purpose	4
11.0.2 Scope	4
11.1 Secure Areas	4
11.1.1 Physical Security Perimeter	4
11.1.2 Physical Entry Controls	5
11.1.3 Securing Offices, Rooms and Facilities.....	6
11.1.4 Protecting against External and Environmental Threats	6
11.1.5 Working in Secure Areas.....	6
11.1.6 Delivery and Loading Areas	6
11.2 Equipment.....	7
11.2.1 Equipment Siting and Protection	7
11.2.2 Supporting Utilities	7
11.2.3 Cabling Security	7
11.2.4 Equipment Maintenance	8
11.2.5 Removal of Assets.....	8
11.2.6 Security of Equipment and Assets Off-Premises.....	8
11.2.7 Secure Disposal or Reuse of Equipment	9
11.2.8 Unattended User Equipment.....	9
11.2.9 Clear Desk and Clear Screen Policy.....	10

11.0 Physical and Environmental Security Policy

11.0.1 Purpose

11.0.1.1 The purpose of the RXO Inc. (RXO) Physical and Environmental Security Policy is to provide information security requirements for the processes related to protecting RXO's secure areas and equipment. Physical security controls addressed in this document include the physical perimeter(s); physical entry controls securing offices, rooms, and facilities; protection against external and environmental threats; and requirements for working in secure delivery and areas.

11.0.2 Scope

11.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all full-time and part-time employees, agents, contractors, and third-party partners, as well as all data and systems used by or supporting the company.

11.0.2.2 This policy encompasses all phases of physical and environmental controls used to secure and protect information assets. The policy applies to all classes of protected information and the systems and environments that store, process or transmit such information.

11.1 Secure Areas

11.1.1 Physical Security Perimeter

11.1.1.1 Security perimeters must be defined and used to protect areas that contain either sensitive, critical information, or information processing facilities.

11.1.1.1.A Each RXO location used to store, process or transmit sensitive information must be periodically reviewed and subjected to risk assessment activities. The security requirements regarding assets within the perimeter must then be defined based upon the outcome of these reviews.

11.1.1.1.B Perimeters of a building or site containing information processing facilities must be physically sound (i.e., there must be no gaps in the perimeter or areas where a break-in could easily occur). Roofs, walls, and flooring must be of solid construction, and all external portals (e.g., doors, windows, loading bays, etc.) must be suitably protected against unauthorized access with control mechanisms (e.g., bars, alarms, and locks). All entry points into the facilities must be locked when unattended, and external protection must be considered for windows, particularly at ground level.

11.1.1.1.C Staffed reception areas, access control cards on elevators and entrance doors, physical door locks, or other, equivalent means to control physical access to the site or building, must be used to restrict access to authorized personnel. Where applicable, physical barriers must be established to prevent unauthorized physical access and environmental contamination.

11.1.1.1.D All fire doors and walls must be alarmed, monitored and tested to ensure that they are in accordance with the local fire code and the level(s) of resistance established by regional, national and, where needed, international standards.

11.1.1.1.E Physical intrusion detection systems must be installed according to the results from individual facility risk assessments. Automated control systems must be continuously monitored by security personnel, have logging enabled, and the logs must be retained and reviewed in alignment with RXO practices. These controls must be regularly tested to ensure appropriate functionality for, at a minimum, all external doors, and accessible windows, unoccupied areas and other sensitive areas (e.g., computer room or communications rooms).

11.1.1.1.F The physical perimeters of the Information processing facilities managed by RXO must either be physically separate from those managed by external parties or sufficient contractual obligations must exist to ensure that equivalent levels of expected controls are implemented by the third parties.

11.1.2 Physical Entry Controls

11.1.2.1 Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

11.1.2.1.A Physical entry access controls must be implemented to a level of rigor that corresponds with the sensitivity of the activities performed within the facility. Access should only be granted for specific, authorized purposes, and the identity of visitors must be authenticated by appropriate means.

11.1.2.1.B All identification badges for visitors, contracted personnel, and RXO personnel must be always worn visibly at or above the waist by all persons. Visitors must be badged with printed "Visitor: badges, escorted, and supervised at all times in controlled areas. Authorized contracted personnel must wear photo badges as a requirement of granting limited access to non-controlled areas. All RXO personnel must wear photo badges without regard to whether they are granted access to controlled areas including data centers and sensitive areas. All visitors must be provided verbal or written instructions on the security requirements of the areas and on the appropriate emergency procedures.

11.1.2.1.C Access to areas where processing or storage of confidential information must be restricted to only authorized individuals via implementation of appropriate access authentication controls. Third party support service personnel must only be granted restricted access to secure areas or confidential information processing facilities when required, with access authorized, and monitored.

11.1.2.1.D A physical or electronic audit trail of all access to sensitive locations must be implemented, securely maintained, and regularly monitored, with the date and time of entries and departures recorded.

11.1.2.1.E All employees, contractors and external visitors must wear RXO approved forms of visible identification that indicates whether they are an employee, contractor, or visitor. Where applicable, allowed dates of admission may be specified on the identification. In the event an unauthorized or un-badged person is detected, employees are expected to immediately escort the person or identify the person to available management members or notify security personnel.

11.1.2.1.F Access rights to secure areas must be regularly reviewed, updated, and revoked when necessary.

11.1.3 Securing Offices, Rooms and Facilities

11.1.3.1 Physical security for offices, rooms, and facilities must be designed and applied.

11.1.3.1.A Security controls governing physical security for offices, rooms and facilities must be implemented to ensure that these facilities are properly protected to minimize exposure to unauthorized access. Where applicable, buildings must be unobtrusive and give a minimum indication, outside or inside the building, of the presence of information processing activities. Facilities must be constructed and arranged in a manner that prevents confidential information or activities from being observed by unauthorized personnel. Directories and internal telephone books identifying locations of confidential information processing facilities must not be readily accessible to unauthorized visitors.

11.1.4 Protecting against External and Environmental Threats

11.1.4.1 Physical protection against natural disasters, malicious attacks, or accidents must be designed and applied.

11.1.4.1.A Facilities containing or supporting critical business processes must be protected from external and environmental threats. The threats to be addressed must be determined as part of periodic risk assessment(s), and should include, at a minimum, damage from fire, flood, earthquake, explosion, civil unrest and other forms of disaster, natural or man-made. Where third party facilities are used, only reputable firms and/or those able to provide evidence of professional qualification, i.e., professional license and/or certifications, should be considered.

11.1.5 Working in Secure Areas

11.1.5.1 Procedures for working in secure areas must be designed and applied.

11.1.5.1.A Procedures for employees and third-party service providers/contractors working in secure areas must be developed, documented, and implemented to provide applicable controls that govern working in secure areas. Personnel must only be aware of the existence of, or activities within, a secure area on a need-to-know basis. Unsupervised working in secure areas must be avoided both for safety reasons and to prevent opportunities for malicious activities. Vacant secure areas must be physically locked and periodically monitored. Personal photographic, video, audio, or other recording equipment, such as cameras in mobile devices, must not be permitted within secure working areas unless specifically authorized.

11.1.6 Delivery and Loading Areas

11.1.6.1 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

11.1.6.1.A All delivery and loading areas must be designed with consideration of security controls that minimize risk factors.

11.2 Equipment

11.2.1 Equipment Siting and Protection

11.2.1.1 Equipment must be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

11.2.1.1.A As part of the design criteria used to protect sensitive processing facilities, specific equipment security controls must be implemented to site and protect equipment from environmental threats, environmental hazards, and opportunities for unauthorized access.

11.2.1.1.B Setup of information processing facilities used to handle sensitive data must consider the location of the equipment carefully to reduce the risk of information accessibility by unauthorized persons during use. The selection of equipment location must minimize unnecessary access into work areas. Storage facilities must be secured to avoid unauthorized access.

11.2.1.1.C Controls must be implemented in a fashion that provides acceptable protection to address potential physical and environmental threats (e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism).

11.2.1.1.D Guidelines must govern eating, drinking, and smoking in proximity to information processing facilities. Additionally, environmental conditions, such as temperature and humidity, must be monitored for conditions which could adversely affect the operation of information processing facilities. All facilities must be protected from power surges, include lightning protection filters fitted to all incoming power and communications lines, employ general lightning protection, and where necessary, make use of protections that minimize the risk of information leakage due to electromagnetic emanation.

11.2.2 Supporting Utilities

11.2.2.1 Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

11.2.2.1.A Supporting utilities (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) must conform to equipment manufacturer's specifications and local legal requirements, undergo regular reviews to validate their capacity to meet current needs and expected business growth, as well as interactions with other supporting utilities, be inspected and tested regularly to verify proper functionality, be configured to generate alarms in the event of malfunctions and if necessary, have multiple feeds with diverse physical routing.

11.2.2.1.B Emergency lighting, communications and emergency switches, and valves to cut off power, water, gas, or other utilities location must be located near emergency exits or equipment rooms.

11.2.3 Cabling Security

11.2.3.1 Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference, or damage.

11.2.3.1.A Power and telecommunications cabling carrying data or supporting information services must be adequately protected. Power cables must be segregated from communications cables to prevent interference. In addition, cabling supporting sensitive or critical systems must be reviewed to determine if additional controls are necessary.

11.2.4 Equipment Maintenance

11.2.4.1 Equipment must be correctly maintained to ensure its continued availability and integrity.

11.2.4.1.A Security controls for equipment maintenance must be implemented to ensure that maintenance activities are properly scheduled and executed in accordance with the service intervals and specifications provided by the vendors, only authorized maintenance personnel perform inspections or repairs to the service equipment and records of all faults and maintenance are documented and available for inspection.

11.2.4.1.B Appropriate controls must be implemented when equipment is scheduled for maintenance, considering whether this maintenance is performed by personnel on site or external to the company. When required, confidential information must be removed from equipment accessed by third parties or maintenance personnel.

11.2.4.1.C All equipment maintenance requirements must incorporate appropriate security controls to ensure that the applied procedures and oversight fully support required compliance and insurance obligations. Equipment inspections must ensure that the equipment has not been tampered with and is fully functional within operational specifications prior to putting equipment back into operation after its maintenance.

11.2.4.1.D Periodic inspection of equipment must be conducted to validate capability, suitability and compliance (e.g., fire extinguishers, sprinklers, alarm systems, surveillance recording equipment firmware, UPS battery life, etc.).

11.2.4.1.E Review of assets must also ascertain that all media and equipment is current with the asset management records.

11.2.5 Removal of Assets

11.2.5.1 Equipment, information or software must not be taken off-site without prior authorization.

11.2.5.1.A Internal and external party users must receive formal approval prior to removing assets to off-site locations. Time limits governing the allowed periods for asset removal must be set and returns regularly monitored to ensure compliance. Where necessary and appropriate, records must be maintained of all removed assets that include removal dates, proof of authorization and return dates. Additionally, the identity, role, and affiliation of anyone who handles or uses assets must be documented, and this documentation returned with the equipment, information, or software.

11.2.6 Security of Equipment and Assets Off-Premises

11.2.6.1 Security must be applied to off-site assets, considering the different risks of working outside the company's premises.

11.2.6.1.A The use of any information storing and processing equipment outside the company's premises must be authorized by management. This applies both to the equipment owned by RXO

as well as equipment owned privately and used on behalf of RXO. Additionally, equipment and media taken off premises must not be left unattended in public places.

11.2.6.1.B Users must always comply with manufacturers' instructions for protecting equipment (e.g., protection against exposure to strong electromagnetic fields).

11.2.6.1.C All off-premises locations (including temporary work sites must be subjected to periodic risk assessments to determine the appropriate control application, such as lockable filing cabinets, clear desk policy, access controls for computers and secure communication within the office. RXO will not inspect homes and teleworking environments but will provide employees and contractors guidance for the use of lockable filing cabinets, clear desk policy, access controls for computers, and secure communication within their work environment. Risks may vary considerably between locations, and consideration of these unique risks must be considered in determining the most appropriate controls.

11.2.6.1.D All equipment taken off-premises in the custody of more than one individual or external party must be reflected in a chain of custody log that includes, at a minimum, the names and companies of anyone who becomes responsible for the equipment while off-premises.

11.2.7 Secure Disposal or Reuse of Equipment

11.2.7.1 All items of equipment containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

11.2.7.1.A Users must utilize proper destruction methods when disposing of RXO information. Data Owners are responsible to ensure that media containing "Business Confidential" or more sensitive data must be destroyed or subjected to sanitization methodologies that prevent any form of recovery when it is no longer needed for business or legal reasons.

11.2.7.1.B All media containing sensitive information (e.g., hard drives, tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's, paper, etc.) must be sanitized or disposed of in a manner commensurate with the information contained. At a minimum, these sanitization and destruction methodologies must ensure that any data contained in the media is rendered unable to be restored or recreated.

11.2.7.1.C If the media are to be sanitized or destroyed by a resource outside of RXO, an external recycling service specializing in the destruction corporate information must be used. The agreement governing this work must address confidentiality requirements and adequate security controls for handling sensitive media.

11.2.8 Unattended User Equipment

11.2.8.1 Users must ensure that unattended equipment has appropriate protection.

11.2.8.1.A All users must be made aware of security requirements for protecting unattended equipment, and their responsibilities for implementing such protection.

11.2.8.1.B Equipment (including mobile devices) containing or with access to sensitive data, applications, systems or networks must not be left unattended where unauthorized use or

observation may occur. These devices must be secured by a key lock or an equivalent control (such as password access) when not in use.

11.2.8.1.C All users must terminate or log off from active sessions, applications, or network services when finished unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver).

11.2.9 Clear Desk and Clear Screen Policy

11.2.9.1 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted.

11.2.9.2 This policy must be reviewed annually, or when significant changes occur, to ensure it aligns with evolving threats and business needs.

Certificate of Review

Physical and Environmental Security Policy

December 18th 2025 10:18:48 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Tuesday, November 25, 2025 2:11 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:57 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:18 AM EST